

MAIN MENU:	CALENDAR	SYLLABUS	DISCUSSION	ADMINISTRATION
NOTICES:	The Group Listings have been updated to reflect the final class list. Be sure to find your name on the list.			

## eContracts IV: Digital Signatures, Digital Enforcement

### READINGS

#### Part I Authentication: the State of Digital Signature Legislation

In a world where contracts are consummated over the Internet, how do you formally signify your assent to the terms? Equally importantly, how do you prove that you are who you say you are?

Demonstrating that you "are who you say" is generally known as "authentication". The most common form of authentication, of course, is the **signature**. Its counterpart in the online context is -- happily -- the "digital signature".

Digital signatures are commercially available today. One developer, Verisign, describes them this way (from <http://digitalid.verisign.com/client/help/introSignature.htm>):

#### What is a digital signature?

A digital signature functions for electronic documents like a handwritten signature does for printed documents. The signature is an unforgeable piece of data that asserts that a named person wrote or otherwise agreed to the document to which the signature is attached.

A digital signature actually provides a greater degree of security than a handwritten signature. The recipient of a digitally signed message can verify both that the message originated from the person whose signature is attached and that the message has not been altered either intentionally or accidentally since it was signed. Furthermore, secure digital signatures cannot be repudiated; the signer of a document cannot later disown it by claiming the signature was forged.

In other words, digital signatures enable "authentication" of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.

#### How is a digital signature used for authentication?

Suppose Alice wants to send a signed message to Bob. She creates a message digest by using a hash function on the message. The message digest serves as a "digital fingerprint" of the message; if any part of the message is modified, the hash function returns a different result. Alice then encrypts the message digest [ ]. This encrypted message digest is the digital signature for the message.

Alice sends both the message and the digital signature to Bob. When Bob receives them, he decrypts the signature [ ], thus revealing the message digest. To verify the message, he then hashes the message with the same hash function Alice used and compares the result to the message digest he received from Alice. If they are exactly equal, Bob can be confident that the message did indeed come from Alice and has not changed since she signed it. If the message digests are not equal, the message either originated elsewhere or was altered after it was signed.

Note that using a digital signature does not encrypt the message itself. If Alice wants to ensure the privacy of the message, she must also encrypt it [ ]. Then only Bob can read the message by decrypting it [ ].

It is not feasible for anyone to either find a message that hashes to a given value or to find two messages that hash to the same value. If either were feasible, an intruder could attach a false message onto Alice's signature. Specific hash functions have been designed to have the property that finding a match is not feasible, and are therefore considered suitable for use in cryptography.

---

### **Legislative Activity**

On June 30, 2000, President Clinton Signed the "Electronic Signatures in Global and National Commerce Act," the terms of which can be seen below:

#### **ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT June 30, 2000.**

[edited version]  
[effective date: October 1, 2000]

#### **SECTION 1. SHORT**

TITLE. This Act may be cited as the ``Electronic Signatures in Global and National Commerce Act''.

#### **TITLE I-- ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE SEC. 101. GENERAL RULE OF VALIDITY.**

(a) In General.--Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce-- (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and

(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

(b) Preservation of Rights and Obligations.--This title does not--

(1) limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in nonelectronic form; or

(2) require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to which it is a party.

(c) Consumer Disclosures.--

(1) Consent to electronic records.--Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer in writing, the use of an electronic record to provide or make available (whichever is required) such information satisfies the requirement that such information be in writing if--

(A) the consumer has affirmatively consented to such use and has not withdrawn such consent;

(B) the consumer, prior to consenting, is provided with a clear and conspicuous statement

(i) informing the consumer of

(I) any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties' relationship), or fees in the event of such withdrawal; (ii) informing the consumer of whether the consent applies

(I) only to the particular transaction which gave rise to the obligation to provide the record, or

(II) to identified categories of records that may be provided or made available during the course of the parties' relationship; (iii) describing the procedures the consumer must use to withdraw consent as provided in clause (i) and to update information needed to contact the consumer electronically; and (iv) informing the consumer (I) how, after the consent, the consumer may, upon request, obtain a paper copy of an electronic record, and

(II) whether any fee will be charged for such copy;

(C) the consumer-- (i) prior to consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and (ii) consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent; and

(D) after the consent of a consumer in accordance with subparagraph (A), if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record-- (i) provides the consumer with a statement of

(I) the revised hardware and software requirements for access to and retention of the electronic records, and

(II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and (ii) again complies with subparagraph (C).

rights.-- (A) Preservation of consumer protections.--Nothing in this title affects the content or timing of any disclosure or other record required to be provided or made available to any consumer under any statute, regulation, or other rule of law. (B) Verification or acknowledgment.--If a law that was enacted prior to this Act expressly requires a record to be provided or made available by a specified method that requires verification or acknowledgment of receipt, the record may be provided or made available electronically only if the method used provides verification or acknowledgment of receipt (whichever is required).

(3) Effect of failure to obtain electronic consent or confirmation of consent.--The legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with paragraph (1)(C)(ii).

(4) Prospective effect.--Withdrawal of consent by a consumer shall not affect the legal effectiveness, validity, or enforceability of electronic records provided or made available to that consumer in accordance with paragraph (1) prior to implementation of the consumer's withdrawal of consent. A consumer's withdrawal of consent shall be effective within a reasonable period of time after receipt of the withdrawal by the provider of the record. Failure to comply with paragraph (1)(D) may, at the election of the consumer, be treated as a withdrawal of consent for purposes of this paragraph.

(5) Prior consent.--This subsection does not apply to any records that are provided or made available to a consumer who has consented prior to the effective date of this title to receive such records in electronic form as permitted by any statute, regulation, or other rule of law.

(6) Oral communications.--An oral communication or a recording of an oral communication shall not qualify as an electronic record for purposes of this subsection except as otherwise provided under applicable law. (d) Retention of Contracts and Records.--

(1) Accuracy and accessibility.--If a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or

other record that--

(A) accurately reflects the information set forth in the contract or other record; and (B) remains accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.

(2) Exception.--A requirement to retain a contract or other record in accordance with paragraph (1) does not apply to any information whose sole purpose is to enable the contract or other record to be sent, communicated, or received.

(3) Originals.--If a statute, regulation, or other rule of law requires a contract or other record relating to a transaction in or affecting interstate or foreign commerce to be provided, available, or retained in its original form, or provides consequences if the contract or other record is not provided, available, or retained in its original form, that statute, regulation, or rule of law is satisfied by an electronic record that complies with paragraph (1).

(4) Checks.--If a statute, regulation, or other rule of law requires the retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with paragraph (1).

(e) Accuracy and Ability To Retain Contracts and Other Records.--Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be in writing, the legal effect, validity, or enforceability of an electronic record of such contract or other record may be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.

(f) Proximity.--Nothing in this title affects the proximity required by any statute, regulation, or other rule of law with respect to any warning, notice, disclosure, or other record required to be posted, displayed, or publicly affixed. (g) Notarization and Acknowledgment.--If a statute, regulation, or other rule of law requires a signature or record relating to a transaction in or affecting interstate or foreign commerce to be notarized, acknowledged, verified, or made under oath, that requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.

(h) Electronic Agents.--A contract or other record relating to a transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound.

(i) Insurance.--It is the specific intent of the Congress that this title and title II apply to the business of insurance.

(j) Insurance Agents and Brokers.--An insurance agent or broker acting under the direction of a party that enters into a contract by means of an electronic record or electronic signature may not be held liable for any deficiency in the electronic procedures agreed to by the parties under that contract if-- (1) the agent or broker has not engaged in negligent, reckless, or intentional tortious conduct; (2) the agent or broker was not involved in the development or establishment of such electronic procedures; and (3) the agent or broker did not deviate from such procedures.

## State Initiatives

Many, though not all, states have passed legislation authorizing digital signatures.

*McBride, Baker & Coles LLP, E-Commerce Spotlight (Digital Signatures)* (2001) (summary table) for further information, including state-by-state details, see *McBride, Baker & Coles LLP, Ecommerce Spotlight (Digital Signatures)* (2001) (overview).

## The International Aspects

*Internet Law & Policy Forum, An Analysis of International Electronic and Digital Signature Implementation (September 2000)* (summary report)

---

### Opposition to Digital Signatures

While digital signatures seem like an easy issue to support, it is worth noting that there remains at least some opposition.

One commentator has noted that digital signature legislation doesn't solve the current mess of standards relating to digital signatures, and that digital signatures may leave the "unconnected" (those without access to the net) behind.

*Jesse Berst, Sign of Trouble: The Problem With E-Signatures, ZD Net AnchorDesk, July 17, 2000*

The Consumer Project on Technology, a group affiliated with Ralph Nader, has issued the following statement about the Federal "E-Sign" Act:

People should understand that this bill is about legal issues. It does not create any new technology. The bill was pushed to solve the problems of businesses, and not to protect consumers. The legislation will increase the risks of identity theft. According to the National Consumer Law Center, the bill places new burdens on consumers to provide evidence in disputes over electronic transactions.

The E-sign Act increases the legal obligations on consumers who interact with businesses on the Internet and through other digital media.

The E-sign Act raises the legal status of agreements that are 'signed' using electronic technologies, including such authorizations as click-on buttons on web pages, as well as many other electronic authorizations, of varying degrees of security. On the one hand, it overrides other statutes and regulations, and declares as a general rule, that no contract or signature can be denied legal effect, solely on the grounds that it was in electronic form. On the other hand, it fails in important ways to guarantee that consumers will be protected from fraud or unfair business practices in a wide range of matters.

In general, electronic transactions may leave consumers more vulnerable to unauthorized use, compared to conventional transactions. Technology residing on a consumer's personal computer can hardly be expected to be shielded from malicious intrusions. Unlike a handwritten signature, if an electronic authorization is stolen or forged, the legitimate owner will be hard-pressed to prove that it was used fraudulently. The E-sign Act contains no provision to limit the liability of consumers victimized by fraudulent spending.

Congress rejected pleas from consumer groups that the e-sign bill include a provision to ensure that a contract cannot be altered once a consumer's digital signature is affixed. The Senate language on this was dropped from the bill that was signed by the President today. The risk is that consumers will be victimized by changes in contractual text, inadvertent or otherwise, eroding the consumer's ability to reproduce copies of digital contracts at a later date, or admit such documents as evidence.

The digital signature bill is likely to hurt consumers lacking access to the Internet, especially low-income consumers and minorities. The E-sign Act does allow the consumer the choice of receiving a contract in electronic or paper form. However, given the prevalence of adhesion contracts in business-to-consumer transactions, this 'choice' may very well be "take-it-or-leave it," or constrained by penalty fees for paper-based contracting, a practice not prohibited by the legislation.

## NOTES & QUESTIONS

1. The Internet Law & Policy Forum (ILPF) notes three 'categories' of digital signature legislation:

*prescriptive* (requires a certain technology)

*standards-based* (establishes technological standards, but doesn't specify a technology)

*signature-enabling* (silent as to technology issues)

Into which category would you put the "e-sign" act? What are the pros and cons of each of these categories? Which would you choose as a legislator?

2. Consider the infrastructure required to operate a digital signature system. That is, in the example above, who decides that Alice is actually who she says she is? (And who gives that person / organization the authority to do so?)

This issue is addressed by the use of Certificate Authorities (CAs), who distribute and authenticate digital signatures. At this point, there are many certificate authorities -- all private corporations, operating without licensing or regulation. Do you think this can/will continue? Are there legal risks involved with being a certificate authority?

COPYRIGHT © 2001 R. POLK WAGNER.



Firm

Practice Areas

Attorneys

In the News

Recruiting

**E-Commerce  
Spotlight**

E-Commerce  
E-Health  
Recent Updates

Search E-Commerce:

## E-Commerce Spotlight

E-Commerce · Legislative Tables

Overview · [Legislative Tables](#) · [State Initiatives](#) · [Federal Initiatives](#) · [International Initiatives](#) · [Uniform Acts & Other Initiatives](#)



### Laws Authorizing Signatures

State	Bill/Statute	Type of Signature Authorized	Scope
AL	Alabama Electronic Tax Return Filing Act (1997 AL HB 405)	Electronic Signature (Technology Neutral)	Limited to the electronic filing of tax returns and other documents with the Department of Revenue.
AL	Alabama Uniform Electronic Transaction Act	Electronic Signatures (technology neutral)	Electronic records and electronic signatures relating to a transaction
AK	1997 Alaska Senate Bill 232 - Act relating to electronic signatures, electronic records and public records	Electronic Signatures with specified authentication attributes only (Technology Neutral)	Generally applicable to all communications
AZ	Arizona Administrative Code, Title 2, Ch. 12, Art. 5. "Electronic Signatures"	Electronic Signatures (Technology Neutral)	Arizona Administrative Code
AZ	Arizona Revised Statutes § 41-121	Electronic Signature (Technology Neutral)	Limited to use by state agencies, and for the acceptance of documents filed with the Secretary of State.
AZ	Arizona Revised Statutes §41-121, §41-132; (1998 Arizona House Bill 2518)	Digital and Electronic Signatures (Technology Specific - PKI)	Limited to documents filed with or by a state agency, board or commission.
AZ	Arizona Revised Statutes, amending § 41-121 (1999 AZ HB 2234)	Electronic Signatures (Technology Neutral)	Limited to documents filed with or by a state agency, board or commission.
AZ	Arizona Uniform Electronic Transactions Act (2000 Arizona House Bill 2069)	Electronic Signatures (Technology Neutral)	Generally applicable to any electronic signature relating to a transaction
AR	Arkansas Code 23-61-107 (1999 Arkansas House Bill 1375)	Electronic Signatures (Technology Neutral)	Limited to communications with the Insurance Commissioner
AR	Arkansas Code: Financial Identity Fraud - 1999 Arkansas House Bill 1167	Electronic Signatures (Includes "Digital Signatures" in the definition of Electronic Signature) - Technology Neutral	Generally applicable to all communications
	Arkansas Electronic		

AR	Records and Signatures Act (1999 Arkansas Senate Bill 418)	Electronic Signatures (Technology Neutral)	Generally applicable to all communications
AR	Arkansas Information Network (1999 Arkansas Senate Bill 378)	Electronic Signatures (Includes "Digital Signatures " in the definition of Electronic Signature) - Technology Neutral	Limited to communications with public entities.
AR	Arkansas Right To Privacy Act (1999 Arkansas Senate Bill 912)	Electronic Signatures (Includes "Digital Signatures " in the definition of Electronic Signature)- Technology Neutral	Digital Signatures, Electronic Identification Numbers, or any other numbers or information that can be used to access a person's financial resources.
AR	Arkansas Tax Procedure Act (1999 Arkansas H.B. 1631)	Electronic Signatures (Includes "Digital Signatures " in the definition of Electronic Signature) - Technology Neutral	Limited to tax returns communicated with Department of Finance and Administration.
AR	Arkansas Uniform Electronic Transactions Act (1999 Arkansas House Bill 1021)	Electronic Signatures; Electronic Transactions	Generally applicable to all transactions.
CA	California Act related to acceptance of electronic signatures by health care industry (1997 California SB 955)	Electronic Signatures (Technology Neutral)	Limited to the acceptance of electronic signatures by health care service plans and insurers.
CA	California Act relating to electronic filing and securities (1997 California Assembly Bill 721)	Electronic Signatures (Technology Neutral)	Limited to the electronic filing of certain securities-related documents.
CA	California Civil Code (1999 California Senate Bill 1124)	Digital and Electronic Signatures (Technology Neutral)	Brokerage agreements
CA	California Code of Regulations Title 2. Division 7. Chapter 10. Digital Signatures	Electronic Signatures with specific attributes only (Technology Neutral)	Limited to establishing the Standards for acceptable digital signatures and certification authorities.
CA	California Education Code s. 70901.1 (1997 California Assembly Bill 521)	Digital Signature (Technology Not Specified)	Limited to the electronic submission of student residency forms.
CA	California Financial Code (1999 California A.B No. 2503)	Digital and Electronic Signatures (Technology Neutral)	Digital signature's and consumer contracts with financial institutions
CA	California Financial Code (1999 California Assembly Bill 583)	Electronic Signatures (Technology Neutral)	Escrow agents and instructions
CA	California Government Code & Code of Civil Procedure (1999 California Senate Bill 367)	Electronic Signatures (Technology Neutral)	Applies to electronic transmission and payment relating to court filings
CA	California Government Code s. 14608 (1993 California Assembly Bill 2887)	Electronic Signatures (Technology Neutral)	Limited to approval or authorization of an act or transaction under California Government Code.
CA	California Government Code s. 16.5 (1995) (1995 California Assembly Bill 1577)	Electronic Signatures (Technology Neutral)	Limited to communications with public entities.
	California		

CA	Government Code s. 25105 (1997 California Assembly Bill 972)	Digital Signature (Technology Not Specified)	Limited to the reproduction of public records.
CA	California Health and Safety Code (1995 California Assembly Bill 2755)	Electronic Signatures (Technology Neutral)	Limited to the electronic filing of certificates of death.
CA	California Online Disclosure Act of 1997 (1997 California Senate Bill 49)	Electronic Signatures (Technology Neutral)	Limited to the electronic filing of reports and statements required under the Political Reform Act of 1974.
CA	California Uniform Electronic Transactions Act (1999 California Senate Bill 820)	Electronic Signatures (Technology Neutral)	any electronic record or electronic signature created, generated, sent, communicated, received, or stored on or after January 1, 2000 (subject to specific exclusions found in s. 1633.3 and other conditions found in the Act)
CO	Colorado Government Electronic Transactions Act (1999 Colorado House Bill 1337)	Electronic Signatures with specified authentication attributes only (Includes "Digital Signatures " in the definition of Electronic Signature) - Technology Neutral	Section 1 is applicable to to electronic records and electronic signatures generated, stored, processed, communicated, or used for any governmental transaction, with exceptions; subsequent sections are generally applicable to electronic signatures and rec
CO	Colorado Revised Statutes (1999 Colorado House Bill 1079)	Electronic Signatures (Includes "Digital Signatures " in the definition of Electronic Signature)- Technology Neutral	Generally applicable to all communications.
CO	Colorado Revised Statutes (1999 Colorado House Bill 1372)	Electronic Signatures - Technology Neutral	Applicable to the creation of the Office of Innovation and Technology in the Governor's Office, and making an appropriation in connection therewith.
CO	Colorado Revised Statutes § 4-9-413 (1997 Colorado Senate Bill 155)	Electronic Signature (Technology Neutral)	Limited to the electronic filing of UCC financing statements, termination statements, separate statements of assignment, statements of release of collateral, and amendments thereto which delete collateral covered by such statements.
CO	Colorado State Information Technology Governance	Electronic Signature	Rules and policies regarding the use of electronic signatures.
CT	Connecticut Electronic Records and Signatures Act (1999 Connecticut House Bill 6592)	Electronic Signatures (Technology Neutral)	Generally to encourage electronic commerce and other electronic transactions in Connecticut by promoting the use of electronic records and signatures.
DE	Delaware Uniform Electronic Transactions Act (1999 Delaware House Bill 492)	Electronic Signatures (Technology Neutral)	Electronic records and electronic signatures relating to a transaction
DC	No enacted legislation on record		
FL	Florida - House Bill 665	Electronic Signatures	Public Record Plans
FL	Florida Electronic Signature Act of 1996, (1996 Florida	Digital and Electronic Signatures (Technology	Generally applicable to all communications

	Senate Bill 942)	Specific - PKI)	
FL	Florida Statutes, amending Ch. 117 (1998 Florida House Bill 1125)	Digital Signatures (Technology Not Specified)	Notaries Public
FL	Florida Statutes, amending Ch. 117, 471 & 472 (1997 Florida House Bill 1413)	Digital Signatures (Technology Not Specified)	Applies to electronic notarizations and to the electronic public filing of engineering-related documents.
FL	Florida Statutes, amending ss. 15.16 and 607.01401 (1999 Florida Senate Bill 1830)	Electronic Signatures (Technology Neutral)	Limited to filings with the Secretary of State
FL	Florida Uniform Electronic Transactions Act (2000 Florida Senate Bill 1334)	Electronic Signatures (Technology Neutral)	Any electronic record or electronic signature created, generated, sent, communicated, received, or stored on or after July 1, 2000.
GA	2001 Georgia Senate Bill 24	Electronic signatures and records	Amends Code Section 10-12-4 of the Official Code of Georgia Annotated
GA	Georgia Annotated Official Code (1999 Georgia House Bill 312)	Electronic Signatures (Technology Neutral)	Limited to real estate transactions and real estate appraisers
GA	Georgia Annotated Official Code (1999 Georgia Senate Bill 61)	Electronic Signatures (Technology Neutral)	Generally applicable all communications
GA	Georgia Annotated Official Code (1999 Georgia Senate Bill 62)	Electronic Signatures (Technology Neutral)	Generally applicable to all communications, with specific exclusions
GA	Georgia Annotated Official Code (2000 Georgia House Bill 1265)	Electronic Signatures (Technology Neutral)	Limited to returns of and ad valorem taxation of property
GA	Georgia Annotated Official Code (2000 Georgia Senate Bill 465)	Electronic signatures	Limited to the authority of the Georgia Technology Authority
GA	Georgia Electronic Records and Signatures Act (1997 Georgia Senate Bill 103)	Electronic signatures	Generally applicable all communications
GA	Georgia Personal Financial Security Act, (1997 Georgia Senate Bill 513)	Digital Signatures (Technology Not Specified)	Criminal offense of financial identity fraud
HI	Hawaii Uniform Electronic Transactions Act (1999 Hawaii House Bill 2585)	Electronic Signatures (Technology Neutral)	Electronic records and signatures relating to any transaction
ID	Idaho Electronic Signature and Filing Act (1998 Idaho Senate Bill 1496)	Electronic Signatures with specific attributes only (Technology Neutral)	Limited to the filing and issuing of documents by and with state and local agencies.
ID	Idaho Shareholders Proxy Rights	Electronic Signature	Writing authorizing another person or persons to act for the shareholder as proxy.
ID	Idaho Uniform Electronic Transaction Act (2000 Idaho Senate	Electronic Signatures (Technology Neutral)	Electronic records and signatures relating to a transaction

	Bill 1334)		
IL	2001 General Revisory Act	Electronic Signatures	Exemptions
IL	Illinois Vehicle Code Amendment (1999 IL HB 3420)	Electronic Signatures (Technology Neutral)	Amends Section 5 of the Illinois Vehicle Code
IL	Illinois Electronic Commerce Security Act (1997 Illinois House Bill 3180)	Digital and Electronic Signatures (Technology Specific - PKI)	Generally applicable to all communications
IL	Illinois Financial Institutions Digital Signature Act; (1997 Illinois House Bill 597)	Electronic Signatures (Includes "Digital Signatures " in the definition of Electronic Signature) - Technology Neutral	Limited to communications with financial institutions
IL	Illinois General Revisory Act (1999 Illinois Senate Bill 745)	Electronic Signatures (Uses "Digital Signatures " and Electronic Signature interchangeably)- Technology Neutral	Limited to revising the law by combining multiple enactments and making technical corrections.
IL	Illinois State Comptroller Act (1997 Illinois Senate Bill 516)	Electronic Signatures (Uses "Digital Signatures " and Electronic Signature interchangeably)- Technology Neutral	Communications between a state agency and the comptroller
IN	Indiana Code Annotated Electronic Digital Signature Act	Digital signatures	Applies to the state or a state agency other than the judicial branch, legislative branch, and educational institutions.
IN	Indiana Bill amending Indiana Code concerning commercial law (2001 Indiana Senate Bill 46)	Electronic signatures	Electronic records and electronic signatures that relate to a transaction
IN	Indiana Motor Vehicle Electronic Records	Digital Signatures	Electronic record of the Bureau of Motor Vehicles bearing an electronic signature is admissible in a court proceeding.
IN	Indiana Uniform Electronic Transactions Act 2000 Indiana House Bill 1395	Electronic records and signatures	Electronic records and signatures relating to any transaction
IA	Iowa Code § 48A.13 Relating to Voter registration	Electronic signatures	Limited to voter registration forms
IA	Iowa Electronic Commerce Security Act; (1999 Iowa House Bill 624)	Electronic signatures, secure electronic signatures, and digital signatures	Generally applicable to all communications.
IA	Iowa Uniform Electronic Transactions Act (1999 Iowa House File No. 2205)	Electronic signatures and records	
KS	Kansas Uniform Electronic Transactions Act (2000 Kansas House Bill 2879)	Electronic signatures	Any electronic record or electronic signature created, generated, sent, communicated, received or stored on or after the effective date of this act.
KY	Kentucky Revised Statutes (2000 Kentucky House Bill 939)	Electronic Signatures	Electronic filing of campaign finance information
KY	Kentucky Revised Statutes (1998)	Electronic records and	Generally applicable to all communications, with specific

	Kentucky House Bill 708)	signatures	exclusions
KY	Kentucky Revised Statutes (1998 Kentucky Senate Bill 390)	Electronic signatures	Limited to the use of electronic signatures by state agencies in connection with determinations as to whether state construction contractors should be released from performance bonds.
KY	Kentucky Uniform Electronic Transactions Act (2000 Kentucky House Bill 571)	Electronic records and signatures	Applicable to electronic records and electronic signatures relating to a transaction, with specific exclusions.
LA	Louisiana - Department of Transportation Electronic Transactions	Digital Signatures	Electronic Bids
LA	Louisiana - Senate Bill 973 amending 9:34021	Digital and Electronic Signature	Definitions
LA	Louisiana Revised Statutes (1997 Louisiana Senate Bill 609)	Electronic signatures	Electronic signatures by health care providers on medical records
ME	An Act Conforming Maine Digital Signature Law to Federal Law	Digital Signature	Estate Matters
ME	Maine Act to Clarify Signature requirements on Certain Legal Documents (1999 Maine HB 1451)	Electronic records and signatures	Applies to communications in general
ME	Maine Digital and Electronic Signatures - Title to Real Property	Digital and Electronic Signatures	Durable power of attorney, mortgage or other document affecting title to real property
ME	Maine Digital Signature Act	Digital signatures	Transactions involving a state department, agency, office, board, commission, quasi-independent agency, authority or institution.
ME	Maine Uniform Electronic Transactions Act (1999 Maine Senate Bill 995)	Electronic signatures	Commercial transactions
MD	Maryland Digital Signature Pilot Program(1998 Maryland House Bill 523)	Electronic Signatures	Limited to communications among governmental entities
MD	Maryland Digital Signature Regulations	Digital Signatures	Generally applicable to all communications
MD	Maryland Uniform Computer Information Transactions Act - Implied Warranty Exemption	Electronic records and computer information	Limited to electronic records related to computer information transactions
MD	Maryland Uniform Computer Information Transactions Act (2000 Maryland House Bill 19)	Electronic records and computer information	Limited to electronic records related to computer information transactions
	Maryland Uniform Electronic		Generally applicable to all

MD	Transactions Act (2000 Maryland Senate Bill 3)	Electronic signatures	communications, with specific exclusions
MD	Maryland Uniform Electronic Transactions Act Provision Interaction with E-Sign(HB 519)	Electronic Signatures	Applies to the provisions of the Maryland Uniform Electronic Transactions Act
MA	No enacted legislation on record		
MI	Michigan Uniform Electronic Transactions Act (2000 House Bill 5537)	Electronic signatures	Electronic records and electronic signatures relating to a transaction
MN	Minnesota Electronic Authentication Act (Minnesota Statutes Annotated § 325K )	Digital signatures	Generally applicable to all communications
MN	Minnesota Statutes §16B.05 (1997 Minnesota House Bill 871)	Electronic signatures	Limited to the electronic conduct of state business
MN	Minnesota Uniform Electronic Transactions Act (CHAPTER 371- H.F.No. 3109)	electronic records and signatures	Electronic records and electronic signatures relating to a transaction
MS	Mississippi Business Corporation Act (1997 Mississippi House Bill 1313)	Electronic	Limited to the filing of documents with the Secretary of State
MS	Mississippi Digital Signature Act of 1997 (1997 Mississippi House Bill 752)	Digital signatures	
MO	Missouri Bill related to electronic filing (1998 MO SB 844)	Electronic and digital signatures	Limited to filings with the Secretary of State for certain business organizations
MO	Missouri Digital Signatures Act (1998 Missouri Senate Bill 680)	Electronic and digital signatures	Generally applicable to all communications
MT	Montana Code Annotated (1997 Montana House Bill 468)	Electronic commerce	Limited to the electronic filing of documents with the State.
MT	Montana Electronic Transactions with State and Local Government Units Act (1999 Montana House Bill 188)		Limited to transactions with State Agencies
MT	Montana State Filing act (1999 Montana House Bill 616)	Electronic documents	Limited to the electronic filing of documents with the State
MT	Montana Uniform Electronic Transactions Act (2001 Montana House Bill 234)	Electronic Signatures	Electronic records and electronic signatures relating to a transaction
NE	Nebraska Digital Signatures Act, Nebraska Revised Statutes § 86-1701	Electronic signatures	Generally applies to all communication
NE	Nebraska Electronic Transactions Act	Electronic records and	Electronic records and electronic signatures relating to

	(1999 Nebraska Legislative Bill 929)	signatures	a transaction
NE	Nebraska Regulations for the Digital Signatures Act		
NV	Nevada Bill Governing State Transactions (1997 Nevada Senate Bill 42)	Electronic signatures	Financial transactions "pertaining to this state"
NV	Nevada Committee on Commerce and Labor (1999 Nevada Assembly Bill 674)	Digital signatures	Generally applies to all commercial transactions
NV	Nevada Revised Statutes Title 14 § 171.03 (1997 Nevada Assembly Bill 386)	Electronic signatures	Documents filed with courts and public agencies
NV	Nevada Revised Statutes: Chapter 720 Title 59 - Electronic Transfers		apply to any transaction for which a digital signature may be used to satisfy a requirement that a document or record be signed or in writing as set forth in NRS 720.160.
NH	New Hampshire Digital Signature Act (1997 New Hampshire Senate Bill 207)	Electronic signatures	Communications between the State and any agency or instrumentality of the State
NH	New Hampshire Laws 22-1998 (1997 New Hampshire House Bill 290)	Digital signatures	Generally applicable to all communications
NH	New Hampshire Laws 382-1998 (1997 New Hampshire Senate Bill 472)	Electronic signatures	Limited to the electronic filing of UCC financing statements, termination statements, separate statements of assignment, statements of release of collateral, and amendments thereto which delete collateral covered by such statements.
NJ	New Jersey Bill concerning the use of electronic and digital processes by the DMV (1999 New Jersey Assembly Bill 3269)	Digital signatures	Limited to electronic processing of motor vehicle transactions
NM	New Mexico Electronic Authentication of Documents Act (1996 New Mexico House Bill 516)	Electronic authentication and digital signatures	Generally applicable to all communications
NM	New Mexico Electronic Authentication of Documents Act (1999 New Mexico Senate Bill 146)	Electronic authentication and digital signatures	Limited to public records and filings
NM	New Mexico Statutes s. 14-3-15.2	Electronic authentication	Public records and filings
NM	New Mexico Uniform Electronic Transaction Act : 2001 New Mexico House Bill 232	Electronic Signatures (Technology Neutral)	Electronic records and electronic signatures relating to a transaction
	New York Consolidated Laws Chapter 57A The		

NY	State Technology Law (includes Article I: New York Electronic Signatures and Records Act (1999 NY SB 6113))	Electronic and digital signatures	Generally applicable to all communications, with specific exceptions found in § 107.
NY	New York Electronic Signatures and Records Act Regulations (9 NYCRR PART 540)	Electronic records and signatures	Generally applicable to standards and procedures governing the use and authentication of electronic signatures and the utilization of electronic records.
NC	North Carolina Electronic Commerce Act: (1998 NC H.B. 1356)	Electronic signatures	Electronic signatures when used in commerce with public agencies
NC	North Carolina Uniform Electronic Transactions Act (2000 Senate Bill 1266 )	Electronic signatures	This Article applies to any electronic record or electronic signature created, generated, sent, communicated, received, or stored on or after the effective date of this Article.
NC	North Carolina Uniform Electronic Transactions Act Amendment 2001 North Carolina Senate Bill 1023	Electronic records and signatures	Amends the North Carolina UETA
ND	North Dakota Uniform Electronic Transactions Act (2001 North Dakota House Bill 1106)	Electronic Signatures	Electronic records and electronic signatures relating to a transaction
ND	North Dakota Information Technology Bill (1999 ND SB 2043)	Information technology implementation and policy	Generally applies to information technologies of North Dakota
ND	North Dakota Information Technology 1999 North Dakota Senate Bill 2043	Information Technology	
OH	Ohio Uniform Electronic Transactions Act (1999 Ohio House Bill 488)	Electronic records and signatures	Electronic records and signatures relating to transactions
OK	Oklahoma Uniform Electronic Transactions Act (1999 OK S.B. 1598)	Electronic signatures	Electronic records and signatures relating to a transaction
OR	Oregon Digital Signatures Act	Digital Signatures	Use of digital signatures by state agencies
OR	Oregon Electronic Signature Act, Oregon Revised Statutes §192.825 et seq. (1997 Oregon House Bill 3046)	Electronic and digital signatures	Generally applies to all transactions
PA	Pennsylvania Uniform Electronic Transactions Act (1999 Pennsylvania Senate Bill 555)	Electronic records and signatures	Electronic records and electronic signatures relating to a transaction.
PR	Puerto Rico Digital Signatures Act S.B. 423, Law 188	Electronic records and signatures	
RI	Rhode Island Uniform Electronic Transactions Act	Electronic records and electronic signatures	Electronic records and signatures relating to a

	(2000 H.B. 7694)		transaction.
SC	South Carolina Electronic Commerce Act (1997 South Carolina Senate Bill 1167)	Electronic signatures	Generally applicable to all communications
SD	South Dakota Uniform Electronic Transactions Act (2000 Senate Bill 193)	Electronic records and signatures	Applicable to electronic records and signatures relating to any transaction.
TN	Tennessee Code Annotated, amending Title 16, Chapter 1, Part 1 and Title 16, Chapter 3, Part 4 (1997 Tennessee House Bill 1718)	Electronic signatures	Use of electronic signatures in signing of pleadings, court orders, judgment orders, or other court documents.
TN	Tennessee Electronic Commerce Act of 2000 (2000 Tennessee House Bill 3250 / 2000 Tennessee Senate Bill 2430)	Electronic records and signatures	Business transactions and use of electronic signatures and records by county officers and public officials.
TN	Tennessee Uniform Electronic Transactions Act : 2001 Tennessee Senate Bill 376	Electronic signatures (technology neutral)	Electronic records and electronic signatures relating to a transaction
TX	Texas Business & Commerce Code § 2.108 (1997 Texas House Bill 984)	Electronic signatures	Limited to communications with public agencies
TX	Texas Business & Commerce Code, amending Ch. 9 (U.C.C., Art. 9) (1999 Texas Senate Bill 1058)	Digital signatures	Secured transactions
TX	Texas Digital Signature Rule		
TX	Texas Uniform Electronic Transactions Act (UETA)	Electronic Signatures (technology neutral)	Electronic records and electronic signatures relating to a transaction.
UT	Utah Act Relating To Providing Government Services Electronically (2000 HB 90)	Electronic records	Limited to government services
UT	Utah Bill amending Section 46-3-104 of the Digital Signature Act (2000 Utah Senate Bill 76)	Digital signatures	Amends the Digital Signature Act
UT	Utah Digital Signature Act, Utah Code Annotated §§ 46-3-101 to -504	Digital signatures	Generally applicable to all communications
UT	Utah Digital Signature Administrative Rules	Digital signatures	Generally applicable to all communications.
UT	Utah Notaries Public Reform Act - Utah Code § 46-1-1 et seq.	Digital signatures	Limited to notaries public
UT	Utah Uniform Electronic Transactions Act	Electronic records and electronic signatures	Applies to electronic records and electronic signatures relating to a transaction.

	(Senate Bill 125)		
VT	Vermont Act relating to record documents (1997 Vermont Senate Bill 232)	Electronic signatures	Use of electronic signatures in Vermont Land Records
VA	Virginia Electronic Transactions Act ; technical amendments 2001 HB 2411	Electronic Signatures	Applies to electronic records and electronic signatures relating to a transaction.
VA	Virginia Uniform Computer Information Transactions Act (2000 Virginia House Bill 561; 2000 Virginia Senate Bill 372)	Electronic records and computer information	Limited to electronic records related to computer information transactions.
VA	Virginia Uniform Electronic Transactions Act (2000 Virginia House Bill 499)	Electronic Signatures	Applies generally to electronic records and electronic signatures relating to a transaction, with specific exclusions.
WA	Washington Act relating to fraudulently use of digital signatures and digital certificates	Electronic signatures	Fraudulent use of electronic signatures and certificates
WA	Washington Amendments to the Electronic Authentication Act (1999 WA SB 5962)	Digital signatures and electronic records	Generally applies to all communications
WA	Washington Electronic Authentication Act; Washington Code ch. 19.34	Digital signatures	All communications
WA	Washington Sales and Use Tax Exemption Simplification	Electronic Signature	Relates to the simplification of the sale and use tax exemption application process incorporating electronic signatures.
WV	West Virginia Uniform Electronic Transactions Act	Electronic records and signatures	Electronic records and signatures relating to any transaction.
WI	Wisconsin Statutes s. 137.01 et seq. (1997 Wisconsin Assembly Bill 811)	Enacted June 30, 1998	Generally applicable to all communications
WI	Wisconsin Statutes s. 16.855(23) (1997 Wisconsin Assembly Bill 100)	Digital signatures	Limited to the electronic submission of state construction contracts, bids and proposals to the Department of Administration.
WY	Wyoming Statutes § 9-2-2501 Governmental Electronic Transactions	A key encryption or other identification procedure	Documents filed electronically with the Secretary of State
WY	Wyoming Uniform Electronic Transactions Act	Electronic Signatures	Electronic Signatures & Utilization of Electronic Records





Global Networks, Local Rules

INTERNET LAW AND POLICY FORUM

[About ILPF](#) | [To Join ILPF](#) | [Working Groups and Publications](#) | [Member Resources](#) | [Events](#)

Jurisdiction  
Electronic Authentication  
Self Regulation  
Content Liability

Working Groups and Publications

### An Analysis of International Electronic and Digital Signature Implementation Initiatives

Presentation and International Discussion  
10 September 2000  
San Francisco, California

The ILPF invites public comment on this report.  
Please submit comments to [implementation@ilpf.org](mailto:implementation@ilpf.org)

#### REPORT

On 10 September 2000, members of the Internet Law and Policy Forum and international experts listed at the end of this Report met in San Francisco to hear the first public presentation on an ILPF-commissioned paper, *An Analysis of International Electronic and Digital Signature Implementation Initiatives* (the *International Implementation Survey*)<sup>[1]</sup> and to discuss legal and policy issues raised by the current proliferation of such initiatives.

The *International Implementation Analysis* is the third ILPF-commissioned survey of digital and electronic signature efforts. In 1997 in response to a growing number of differing state legislative initiatives within the United States, the ILPF introduced Legislative Principles for Electronic Authentication (1997), <http://www.ilpf.org/digsig/principles.htm>, then issued a United States Survey (1998), <http://www.ilpf.org/digsig/update.htm>, to track continued state enactments. In February 1999, the ILPF published a second survey, this one international in scope, <http://www.ilpf.org/digsig/survey.htm>, and issued International Consensus Principles, <http://www.ilpf.org/digsig/intlprin.htm>.<sup>[2]</sup> The surveys and principles, particularly the International Consensus Principles, were intended to facilitate the creation of an environment for electronic authentication in which users could be assured of the protections of technological advances and recognition of signatures across state and national boundaries.

A growing number of governments are now passing electronic signature legislation<sup>[3]</sup>: The EU Directive has taken effect, a number of nations have adopted legislation, and work on the UNCITRAL model rules has progressed. In addition, a number of entities - governmental, private industry, and combinations of the two - has begun to draft detailed specifications. Accordingly, the ILPF again commissioned a survey, this time of "implementation" initiatives. The term "implementation" initiatives was broadly defined to include almost any set of detailed criteria, most notably (1) standards for granting enhanced legal effects to a methodology and (2) certification or licensing requirements for service providers.

The ILPF commissioned this latest survey first to catalog as many implementation proposals, public and private, as could be identified, and then to see whether its International Consensus Principles, necessarily a set of high level statements, maintained validity in the context of detailed specificity inherent in many implementation schemes.

The following themes and observations emerged in the presentation and expert, international discussion of this International Implementation Analysis.

#### Presentation of the International Implementation Analysis

Chris Kuner opened the 10 September Session with an overview of the purpose of the *International Implementation Analysis*: to inventory and provide specific analysis of current implementation proposals globally. The resulting detail is set out in Part III, the Appendix to the Analysis. Mr. Kuner emphasized the proliferation of implementation initiatives and voiced his view that the number and kinds of differences among the proposals created a real risk to the use of electronic and digital signatures across borders. The *Analysis* concludes:

*With regard to the number of such implementation schemes, it can be seen from the table (Part III of this paper) that nearly all of the industrialized nations have at least initiated a national accreditation, certification, or standardization scheme for electronic signature products and services. One must ask why so many nationally-based schemes are necessary, and why there is not more reliance on a few, larger-scale schemes that could be tailored for a region, or a particular legal system. One could argue that competition will result among the schemes, leading to a "survival of the fittest", which may well be true to some extent; but at the same time, having nearly every country adopt its own implementation scheme for electronic signatures carries the risk of leading to a patchwork of inconsistent national systems that may well imperil international legal interoperability.*

Stewart Baker then surveyed implementation initiatives against the ILPF Consensus Principles,

and vice versa. His "report card" for governments, reflecting a grading system ranging from "A", the highest rating, to "F" for a failing mark, on legislative electronic signature efforts taken as a whole, was as follows:

<b>ILPF International Consensus Principle</b>	<b>Mark</b>
Removing Barriers to Electronic Authentication	A
Respecting Freedom of Contract	B+
Making Laws Governing Electronic Authentication Consistent Across Jurisdictions	B
Avoiding Discrimination and Erection of Non-Tariff Barriers	C
Allowing for Use of Current or Future Means of Electronic Authentication (Technological Neutrality)	D
Promoting Market-Driven Standards	C

In particular, Mr. Baker noted that registration and licensing requirements can create a disincentive to cross border recognition unless the provider which seeks licensing is heavily capitalized and can comply with registration requirements in multiple jurisdictions. He also noted his view that ISSE standards (Information Security Solutions Europe) reflected more government involvement than usual for an industry-led group. Finally, Mr. Baker offered his opinion that the ILPF should be prepared to modify its International Consensus Principles on technological neutrality and non tariff barriers to allow for a more nuanced approach. In his view, some specification of detail is necessarily a part of the legislative approach in many national laws, particularly for those nations which grant a higher level of legal presumption to some but not all kinds of electronic and digital signatures.

### **Discussion: Themes and Observations**

**Security and the Role of Governments.** Not surprisingly, participants agreed that the need for security of online information would only increase as use of the Internet increased. One participant emphasized the importance of security for e business. As explained, the Internet was designed as a free network for widespread sharing of information. To use so fundamentally open a network for commercial applications such as e commerce would require the technical ability to close or block access to that portion of the network used by a business to conduct its own transactions and communications - much the concept of a virtual private network. In this speaker's view, this need to limit access would be contrary to the original nature of the Net and would ultimately require technical solutions beyond the applications level to make electronic authentication work as a network "access limiting device".

Participants noted that the need for security has been a strong justification for government action in the marketplace. Government designation of the specifics of implementation can be seen as necessary and appropriate to ensure a level of security and trust essential for consumers to embrace electronic commerce, to designate a technology in order to assure widespread use and lower cost, to structure a legal framework which reflects cultural preferences, to regulate (or license) providers of certificate services to consumers, or to set some legally-required levels of duty. Other participants, however, saw a higher level of government involvement in the marketplace as an attempt to create a need for authentication, particularly for consumers, and pull an industry into a current vacuum in the marketplace. The danger of such an approach, noted one participant, is that governments have a tendency to require the design of a Ferrari when a simple and less costly truck would do the job.

A difference of opinion about the appropriate role of government in creating trust is not new. The issue has been fundamental and dialogue has been ongoing, from the beginning of the international conversations on electronic signature legislation. One of the ILPF International Consensus Principles favored a more limited role for governments:

#### **Standards for use of electronic authentication methods or technologies should be market-driven to meet user needs.**

COMMENTARY: Governments should avoid laws that force the private sector to designate a particular technology for electronic authentication. Standards (for example, for technical interoperability) should evolve in response to needs in the commercial market, not by the requirement of government.

Significantly, participants noted one way to balance a purely market-driven approach with a stronger role for government. Appropriate government regulation might be a matter of timing. The most effective sequence might be to grant wide party autonomy to closed systems allowing this market segment to develop on its own. Closed systems are beginning to expand, particularly within an industry, for example, banking, but also for non-industry-specific online exchanges across national boundaries. Speakers urged that these private solutions be allowed to flourish and provide experience to guide further government intervention. The flourishing of "closed" systems would be the "key in the ignition" to drive widespread, cost-effective use of electronic signatures forward. The aggrieved consumer was seen as the wrong starting place from which to consider the role of the government because existing consumer laws are so complex, consumer applications have not yet developed, and consumer protection often calls forth a most zealous response.

**The Need to Distinguish between Technical and Legal Standards.** Participants noted the dialogue on implementation and standards was often confused by a failure to distinguish standards which are proposed to resolve technical issues from those which could be used to specify legal effect. Crafting details necessary to designate the kinds of authentication methodologies entitled to a higher level of legal effect without hindering users' ability to move to more advanced technology remains a challenge. Using detailed standards developed for technological purposes as determinants of legal effect was seen as particularly harmful to technological neutrality, party autonomy and cross border legal interoperability.

In this context, one participant argued for a minimalist approach as the strongest protection for users of digital and electronic signatures. Drafting legislation and regulation with the highest level of abstraction possible would allow courts to exercise maximum discretion to give recognition to a signature user's choice of methodology and intent to be bound. This participant gave voice to the view that too many regulatory requirements would deter rather than encourage the use of electronic signatures.

**Cross Border Issues and the Need for Mutual Recognition.** Agreeing on rules for mutual recognition of signatures across borders<sup>[4]</sup> was seen by many participants as the next important step, but as Chris Kuner noted, even the term "mutual recognition" has different meanings. To some, mutual recognition is more limited. Recognition is only granted if the regulatory scheme from which the signature originates has certain shared characteristics with the regulatory scheme under which mutual recognition is sought. For example, a country which requires licensed providers may only recognize a foreign signature if the foreign provider is similarly licensed in its "home" jurisdiction. Similarly, any mutual recognition scheme should recognize cultural differences, sometimes deeply ingrained. For others, mutual recognition means giving recognition to any foreign signature methodology as long as the methodology is valid in the home jurisdiction, without regard to the similarities or differences between legal frameworks. A third kind of mutual recognition would give effect unless the rules of the home jurisdiction were "profoundly" different.

Efforts are under way in some regions to identify such profound differences and construct the terms of recognition. One participant gave the EU credit for an intra-European model of mutual recognition and suggested that the evolution of that system would provide a valuable model. All agreed that a workable system of mutual recognition would be essential to the growth of cross border electronic commerce.

### Conclusions and Recommendations

ILPF's latest commissioned survey, *An Analysis of International Electronic and Digital Signature Implementation Initiatives*, documents and analyzes a proliferation of standards and licensing initiatives to implement legal recognition of digital and electronic signatures. The level of government participation and intervention in the marketplace reflects differences in goals and culture but at the same time, threatens to create a world in which a user cannot choose a signature methodology or level of security which matches the particular need and may not expect recognition of any choice beyond national or regional boundaries.

Participants at the 10 September Session offered three suggestions for governments to balance the legitimate need for implementation details against the potential excesses of those actions. Governments could

1. Allow the marketplace for and use of authentication technologies in closed systems to develop further before structuring legislative and regulatory requirements based on perceived consumer needs.
2. Recognize the difference between standards designed for technological interoperability and those which define legal effects; and
3. Actively seek to define the terms of broader mutual recognition.

The members of the ILPF wish to express their thanks to Messrs. Kuner and Baker for their work on the *International Implementation Survey* and to the international experts listed below for their contributions to a better understanding of this most complex but important topic.

#### Participating ILPF Members

Oracle Corporation  
Genuity Inc.  
Verisign  
UBS Warburg  
Network Solutions, Inc.  
Securify, Inc.  
Bell Canada  
Fujitsu Limited.  
Telus Corporation  
@Nifty  
Fujitsu, Ltd.  
British Telecom  
Visa International  
Schlumberger Limited  
GE Information Services  
NEC, USA

**Experts** Stewart Baker, Steptoe & Johnson  
Rosa Barcelo, Morrison & Foerster  
Mark Bohannon, Software and Information Industry Association  
Roland Brandel, Morrison & Foerster  
Mauricio Devoto, CENIT  
Peter Ferguson, Industry Canada  
Emily Frye, iWitness, inc.  
Brian Hengesbaugh, US Department of Commerce  
Dr. Ulrich Sandl, Federal Ministry of Economics and Technology, Germany  
Mariana Silveira, National Center for American Free Trade  
Brian Smith, Mayer Brown & Platt  
Graham Smith, Bird & Bird  
Yoshitaka Toui, MITI, Japan  
Kristen Tsois, The Naval Postgraduate School  
Shinje Watanabe, NTT DATA Corporation  
Tomohiko Yamakawa, InfoCom Research Inc

### Endnotes

[1] The *International Implementation Analysis* was undertaken jointly by Chris Kuner of the Brussels Office of Morrison and Foerster LLP and Stewart Baker of the Washington DC office of Steptoe & Johnson LLP.

[2] In addition, a Joint Keidanren/ILPF Workshop on Electronic Signatures and Authentication, November 1999 in Tokyo, Japan brought international expert attention to Japanese legislative proposals, <http://www.ilpf.org/workshop/keidanren.htm>.

[3] See, for example, the *Draft Revised Inventory of Approaches to Authentication and Certification in a Global Networked Society*, DSTI/ICCP/REG(2000)1 for an inventory of OECD member country approaches to authentication.

[4] The term "cross-border" has several meanings in this context. Cross border issues may arise within national boundaries. For example, in both Canada and the United States, areas of law effected by legal recognition of non traditional signatures, for example the laws of evidence (in non-national courts) and contract law may be reserved to provinces or states, respectively. "Cross border" is also used to mean "international", that is, a transaction or communication between actors "in" or legally identified with two separate nations. The EU represents a special subset of "cross border" issues because although those issues are international, they are governed by relevant treaty provisions if the actors are within EU member states.

[About ILPF](#) | [To Join ILPF](#) | [Working Groups & Publications](#)  
[Member Resources](#) | [Events](#) | [Home](#)



To print: [Click here](#) or Select **File** and then **Print** from your browser's menu

-----  
 This story was printed from [AnchorDesk](#),  
 located at <http://www.zdnet.com/anchordesk>.  
 -----

## Sign of Trouble: The Problem With E-Signatures

By *Jesse Berst*, [AnchorDesk](#)

July 16, 2000 9:00 PM PT

URL: <http://www.zdnet.com/anchordesk/stories/story/0,10738,2604099,00.html>

With apologies to Sam Goldwyn, an electronic contract isn't worth the paper it's printed on.

But now under a new federal law, it's just as enforceable.

Note from Jesse: Be careful. E-contracting, and e-signatures will eventually change the way business is done, but they'll be slow to catch on. Businesses will get the first chances to sign on the digital line. Consumers will be last.

The delay is for good reason.

When President Clinton recently signed into law the bill giving your online John Hancock the same force of law as your handwritten signature, ([Click for more](#)), he created a potential avenue for bungling or outright fraud big enough to drive a Brinks truck through. [Click for more](#). He also set the stage for a standards battle that could take years to resolve. Here's a quick look at who is providing e-signing services and hardware, what any signature must do and what the hurdles to widespread adoption are.

### TODAYS E-SIGNATURE PLAYERS

Signature is a pretty loose way to define what we are now coming to call digital signatures. You may never have to sign your name to enter into an electronic contract. You might use a smart card and password, a Web tablet, biometrics or an iris scan. [Click for more](#).

Here's a rundown of who is making and selling digital-signature technology, some of which works independently or in concert with others.

ILumin calls its technology the "digital handshake." It creates a secure environment with all the tools necessary to review, edit, sign and store documents. [Click for more](#).

SignOnline, a silicon startup, will issue its own signatures to customers to use, marrying authenticated digital certificates with secure e-documents. Once signed, documents at SignOnline also go into a secure electronic cabinet. [Click for more](#).

Litronic, also a maker of smart cards, is developing technology that treats a user's eye as a fingerprint. A camera scans the user's iris and matches it up with one on record.

Interlink Electronics sells its ePad, which records more than just the shape of your name. It records the date and time of the signing, and your signature is cryptographically linked to the document and biometrically associated to you.

Much of the heavy lifting in the days ahead will be done by companies such as VeriSign and Entrust Technologies, which have already laid strong foundations in developing the public key infrastructure that is the basis of most digital signatures. [Click for more](#).

### ROLE OF AN E-SIGNATURE

Whatever form it takes, here are three things that are vital to every e-signature:

**Authentication.** Like that illegible scribble you call a signature, you have to be the only one that reproduces it.

**Non-repudiation.** This is what it means to sign your name: You can't back out.

**Data integrity.** Whatever it is you've signed has to be secure and unalterable without your consent. Mortgage papers, business contracts. They're not worth signing if someone can go change the substance of them.

#### WHERE E-SIGNATURES TRIP UP

Just because digital signatures are legal, doesn't mean they're safe or smart. And they're certainly not right around the corner. Here are four things that will trip up the e-sign rush.

**Standards.** The new law says nothing about technology. Any number of companies will say their digital-signature technology is the safest and best. We'll likely discover who is right through trial and error. In the meantime, the details of e-signatures and electronic contracts will almost certainly end up back in court, according to Forrester Research's Frank Prince.

**Real-life applications.** Many businesses hailed the arrival of legal e-signatures. Putting them to work is another question. Businesses will have to buy or build their own public key and encryption infrastructure. Not for everyone.

**Digital divide.** The new law allows companies to charge more to customers who can't or won't go online. Prince thinks this means there won't be much consumer use of e-signatures for another five years. He's right.

**Fraud.** Digital signatures won't do away with criminals. In fact, it will give some of them a new hunting ground. The hackers' pot of gold at the other end of the server just got bigger.

Digital signatures are coming, but they're not here yet. Legal and technical barriers still stand in the way of widespread adoption. And there will be some notable disasters in the early days when somebody's 7-year-old clicks and sells the house or buys a car. When that happens, a pen and paper will seem like pretty nifty technology.

Are you ready to sell a house or buy a car just by clicking? Hit the Talkback button and tell me, or go straight to to my [Berst Alerts](#) forum and hash it out. And be sure to take our quick poll below.

When will you put your first e-signature on something?

- Never. I don't trust it.
- 5 years at least.
- Next year, probably.
- Geez, I've already signed that way. What are you guys waiting for?

**Vote**